BadUSB-C: Revisiting BadUSB with Type-C

Hongyi Lu, Yechang Wu, Shuqing Li, You Lin, Chaozu Zhang
Fengwei Zhang

Southern University of Science and Technology

May 28, 2021

Outline

1. Background
2. Design & Prototype
3. Case Study
4. Limitations
5. Mitigation & Responsible Disclosure
6. Conclusion

The Ubiquitous Peripheral

HIDs

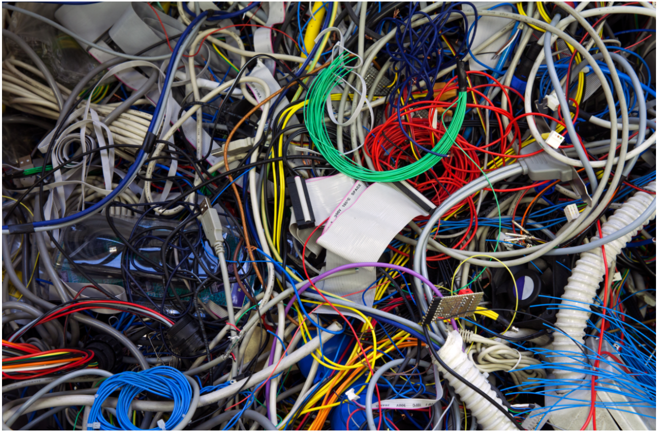
The Ubiquitous Peripheral

Charging

The Ubiquitous Peripheral

Data Transfer

All in One With Type-C



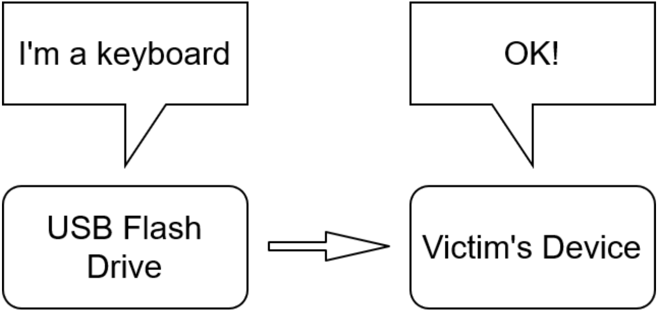
All in One With Type-C

With Great Power Comes Great Responsibility

Year	**Version**	**Peripherals**	**Attacks**
1996	USB 1.x [1, 2]	Keyboard, Mouse...	BadUSB [3]...
2000	USB 2.0 [4]	Flash Drive, CD Driver...	/
2008	USB 3.0 [5]	/	/
2013	USB 3.1 [6]	DisplayPort, ThunderBolt...	**BadUSB-C**
2017	USB 3.2 [7]	/	/

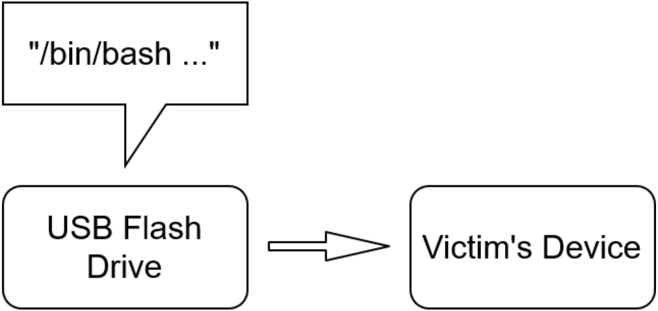
USB Protocol Timeline.

Traditional BadUSB



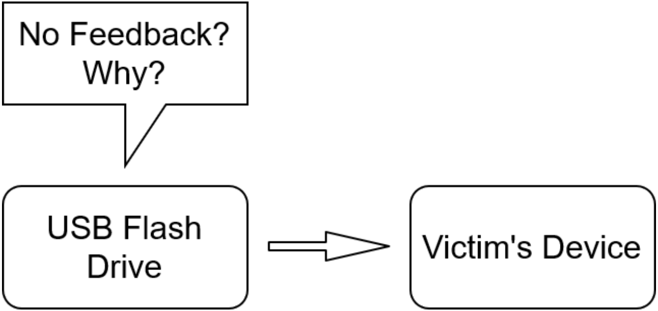
Traditional BadUSB Attack.

Traditional BadUSB



Traditional BadUSB Attack.

Traditional BadUSB



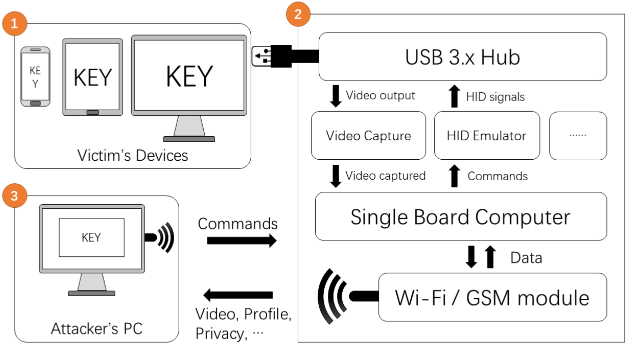
Traditional BadUSB Attack.

BadUSB Limitations

There are some limitations of the traditional BadUSB attack.

- Cannot perform attack precisely.
- Cannot interact with GUI.
- Require host network usage.

Overview

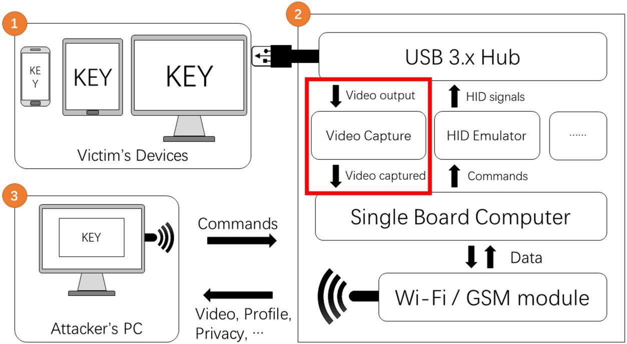


1 Victim's Devices

2 BadUSB-C

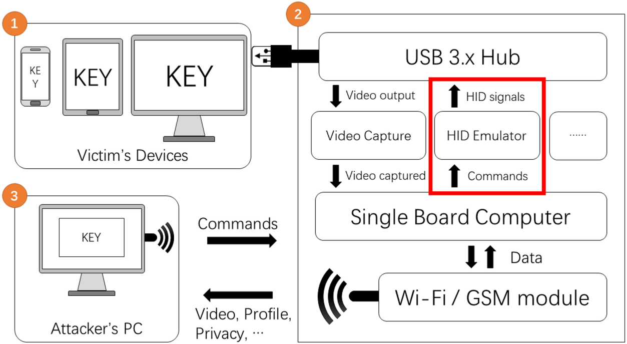
3 Attacker's Remote PC

Video Path



1 Victim's Devices
2 BadUSB-C
3 Attacker's Remote PC

HID Path

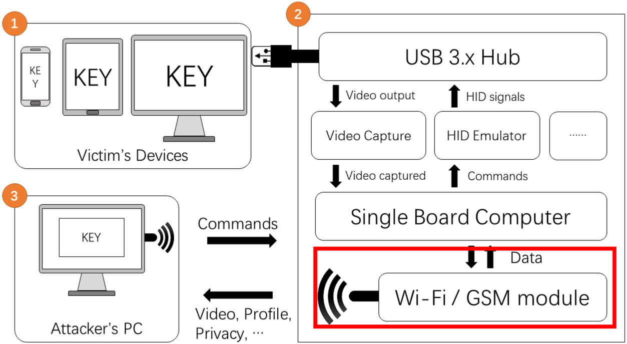


1 Victim's Devices

2 BadUSB-C

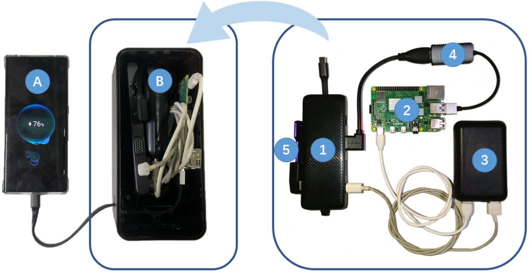
3 Attacker's Remote PC

Individual WiFi/GSM



1 Victim's Devices
2 BadUSB-C
3 Attacker's Remote PC

Prototype



A	Victim’s Device	B	BadUSB-C
1	USB 3.x Hub	2	Raspberry Pi 4B
3	Auxiliary Power Bank	4	Video Capture
5	ATMEGAA32U4 Board		

Sharing Powerbank

Low Power

Sharing Powerbank

Typical Attack Procedure

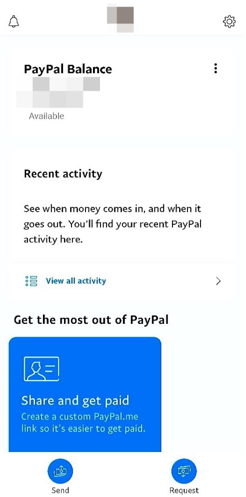
1. The attacker rents a power bank and replaces the internal components with BadUSB-C.
2. An attacker-crafted power bank is returned to the rental station in crowded areas.
3. A user borrows the modified power bank and connects it to his/her own device.
4. The attacker can now fully control the victim’s device.

Experiment Setup

We conducted experiment on a HUAWEI P30 Android smartphone. Eleven applications were selected and tested in the following steps:

1. Login in with a test account.
2. Keep the default settings.
3. Attach BadUSB-C to the test device.
4. Simulate victim's daily usage of the application.

Experiment Screenshots



PayPal Balance

Available

Recent activity

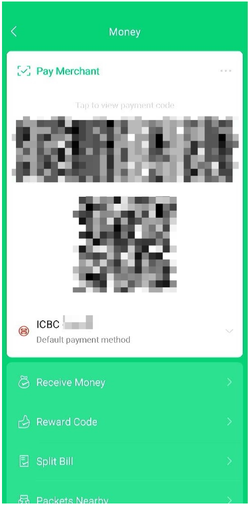
See when money comes in, and when it goes out. You'll find your recent PayPal activity here.

View all activity

Get the most out of PayPal

Share and get paid

Create a custom PayPal.me link so it's easier to get paid.

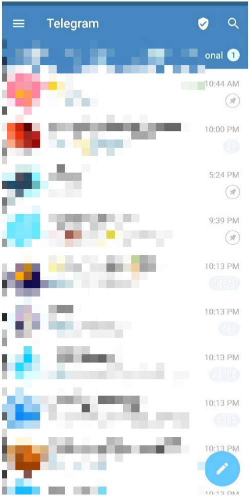


Pay Merchant

Tap to view payment code

ICBC

Default payment method



Experiment Result

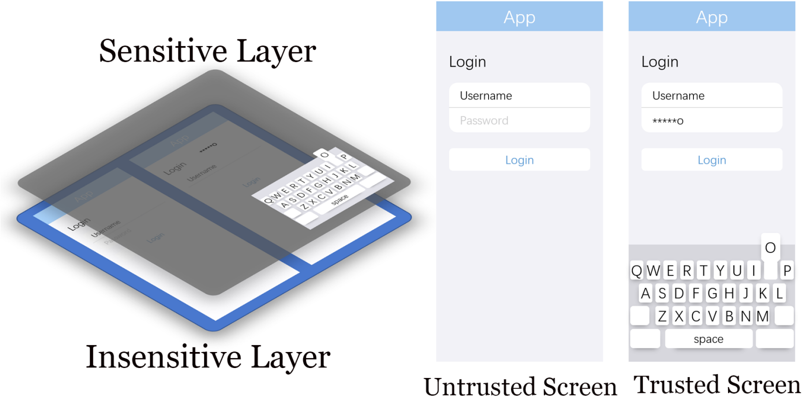
Application	**Leaked Sensitive Information**
WeChat	Financial Status, History, Payment QR Code
WhatsApp	Contacts, Chat History, Phone Number
Alipay	Financial Status, Payment QR Code
Paypal	Paypal Balance
Health	Personal Health Metrics
...	...

Limitations

BadUSB-C also has serveral limitations.

- Cannot bypass biometrics authentications like fingerprint.
- Requires the DisplayPort over USB Type-C feature to work.
- May incur notifications on victim’s devices and be discovered.

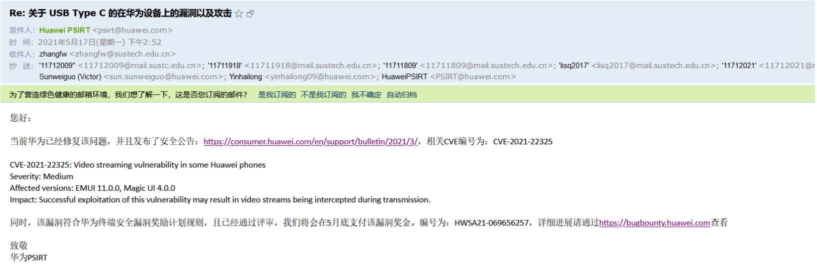
Isolated UI Rendering



Isolated UI Rendering

Responsible Disclosure

We contacted HUAWEI after we discovered this vulnerability, who later assigned a CVE entry (CVE-2021-22325) for this vulnerability.



Re: 关于 USB Type C 的在华为设备上的漏洞以及攻击

发件人：Huawei PSIRT <psirt@huawei.com>
时　间：2021年5月17日(星期一) 下午2:52
收件人：zhangfw <zhangfw@sustech.edu.cn>
抄　送：'11712009" <11712009@mail.sustc.edu.cn>; '11711918' <11711918@mail.sustech.edu.cn>; '11711809' <11711809@mail.sustech.edu.cn>; 'lisq2017' <lisq2017@mail.sustech.edu.cn>; '11712021' <11712021@r
Sunweiguo (Victor) <sun.sunweiguo@huawei.com>; Yinhailong <yinhailong09@huawei.com>; HuaweiPSIRT <PSIRT@huawei.com>

为了营造绿色健康的邮箱环境，我们想了解一下，这是否您订阅的邮件?
是我订阅的
不是我订阅的
我不确定
自动归档

您好：

当前华为已经修复该问题，并且发布了安全公告：https://consumer.huawei.com/en/support/bulletin/2021/3/，相关CVE编号为：CVE-2021-22325

CVE-2021-22325: Video streaming vulnerability in some Huawei phones
Severity: Medium
Affected versions: EMUI 11.0.0, Magic UI 4.0.0
Impact: Successful exploitation of this vulnerability may result in video streams being intercepted during transmission.

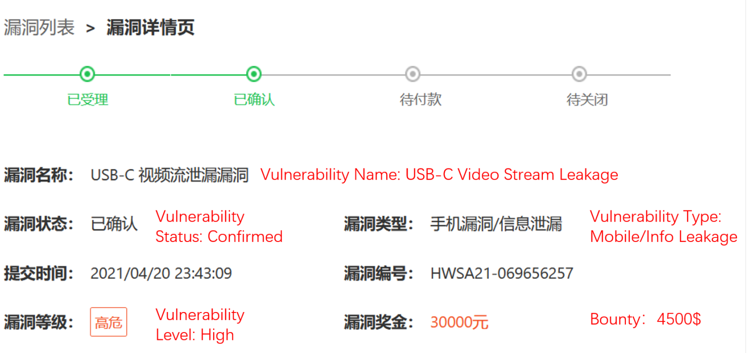
同时，该漏洞符合华为终端安全漏洞奖励计划规则，且已经通过评审，我们将会在5月底支付该漏洞奖金。编号为：HWSA21-069656257，详细进展请通过https://bugbounty.huawei.com查看

致敬
华为PSIRT

HUAWEI Response

HUAWEI Bug Bounty

We also applied for the bug bounty program of HUAWEI and gained a reward of over $4500.



漏洞列表 > **漏洞详情页**

漏洞名称： USB-C 视频流泄漏漏洞 Vulnerability Name: USB-C Video Stream Leakage

漏洞状态： 已确认 Vulnerability Status: Confirmed

漏洞类型： 手机漏洞/信息泄漏 Vulnerability Type: Mobile/Info Leakage

提交时间： 2021/04/20 23:43:09

漏洞编号： HWSA21-069656257

漏洞等级： 高危 Vulnerability Level: High

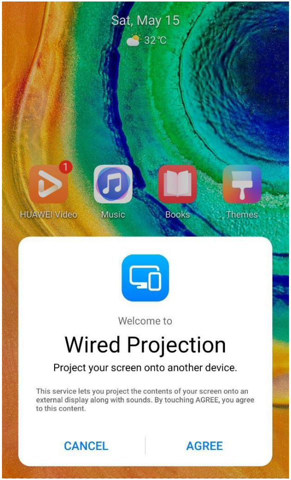
漏洞奖金： 30000元 Bounty：4500$

HUAWEI Bug Bounty

Current Mitigation

Now, mitigation for this vulnerability has already been deployed.

This mitigation requires user authentication before allowing external USB devices.



Welcome to

Wired Projection

Project your screen onto another device.

This service lets you project the contents of your screen onto an external display along with sounds. By touching AGREE, you agree to this content.

Conclusion

We summarize our work as follows.

1. We explore a new attack scheme leveraging the latest feature of USB protocol.
2. We conduct real-life scenario study of sharing powerbank to test BadUSB-C efficiency.
3. We propose novel mitigation for our BadUSB-C attack.

Thank You!

{11712009,11711918,lisq2017,11711809,11712021}@mail.sustech.edu.cn
zhangfw@sustech.edu.cn

- Compaq, D. E. Corporation, I. P. Company, Intel, Microsoft, NEC, and N. Telecom., *Universal Serial Bus Specification, Revision 1.0*, January 1996.

- ——, *Universal Serial Bus Specification, Revision 1.1*, September 1998.

- K. Nohl and J. Lell, “Badusb-on accessories that turn evil,” *Black Hat USA*, vol. 1, no. 9, pp. 1–22, 2014.

- Compaq, D. E. Corporation, I. P. Company, Intel, Microsoft, NEC, and N. Telecom., *Universal Serial Bus Specification, Revision 2.0*, April 2000.

- I. HP *et al.*, “Universal serial bus 3.0 specification,” 2008.

- ——, “Universal serial bus 3.1 specification,” 2013.

I. M. R. S. Apple, Hewlett-Packard and T. Instruments., “Universal serial bus 3.2 specification,” 2017.